AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE	PAGE OF PAGES	
12	1	4

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. *(If applicable)*
116	August 20, 2007	N/A	

6. ISSUED BY	CODE	7. ADMINISTERED BY *(If other than Item 6)*	CODE
Procurement Office George C. Marshall Space Flight Center National Aeronautics and Space Administration Marshall Space Flight Center, AL 35812	PS31-J	Jeffrey S. Jackson (256) 544-8935 Phone (256) 544-3223 Fax	PS31-J

8. NAME AND ADDRESS OF CONTRACTOR *(No., street, county, State, and Zip Code)*	(✓)	9A. AMENDMENT OF SOLICITATION NO.
Science Applications International Corporation (SAIC) Company 6, Technology Services Company 10260 Campus Point Drive San Diego, CA 92121 c/o 6725 Odyssey Drive, Huntsville, AL 35806		9B. DATED *(SEE ITEM 11)*
	X	10A. MODIFICATION OF CONTRACT/ORDER NO. NNM04AA02C
		10B. DATED *(SEE ITEM 13)* 1/1/04

CODE CAGE- 0T5L1 FACILITY CODE SAP- 103429

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

[ ] The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers [ ] is extended, [ ] is not extended.

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods:

(a) By completing Items 8 and 15 and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA *(If required)*
N/A

13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS, IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

(✓)	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: *(Specify authority)* THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES *(such as changes in paying office, appropriation data, etc.)* SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
X	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF: FAR 43.103(a), Procurement Notice 04-25, and Mutual Agreement
	D. OTHER *(Specify type of modification and authority)*

E. IMPORTANT: Contractor [ ] is not, [X] is required to sign this document and return 3 copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION *(Organized by UCF section headings, including solicitation/contract subject matter where feasible.)*

	Negotiated Estimated Cost	Shared Savings Fee	Award Fee Earned	Potential Award Fee	Contract Value	Total Sum Allotted
Prev. Base Total	(b)(4)		$28,307,778	(b)(4)		$745,850,812
This Modification			$0			$0
Rev. Base Total			$28,307,778			$745,850,812

SEE PAGE 2 FOR DESCRIPTION OF AMENDMENT/MODIFICATION

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect

15A. NAME AND TITLE OF SIGNER *(Type or print)*		16A. NAME AND TITLE OF CONTRACTING OFFICER *(Type or print)*	
Jill C. Watkins, Senior Contracts Manager		Jeffrey S. Jackson, Contracting Officer	
15B. CONTRACTOR/OFFEROR	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA	16C. DATE SIGNED
/s/ Jill C. Watkins *(Signature of person authorized to sign)*	August 20, 2007	BY ***/s/ Jeffrey S. Jackson*** *(Signature of Contracting Officer)*	August 20, 2007

STANDARD FORM 30 (Rev. 10-83)
Prescribed by GSA
FAR (48 CFR) 53.243

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT
(continued)

The purpose of this modification is to update Section I, Contract Clauses, to reflect a May 2007 update to the clause entitled "Security Requirements for Unclassified Information Technology Resources" pursuant to the requirements of Procurement Notice 04-25 dated June 19, 2007. As a result, Attachment J-1, Performance Work Statement, is revised to reflect the additional requirements necessitating the documentation submissions resulting from the update of this clause. In addition, Attachment J-2, Data Procurement Document, is also revised to reflect the additional documentation requirements resulting from this update and the deletion of one deliverable replaced by these requirements. Finally, Attachment J-10, Applicable Regulations and Procedures, is revised to reflect the additional procedural requirements relevant to these changes. Accordingly, NNM04AA02C is modified as follows:

A. Under Section I, Contract Clauses, Part B, NASA/FAR Supplement (48 CFR Chapter 18) Clauses, NFS Clause 1852.204-76, Security Requirements for Unclassified Information Technology Resources, is revised to reflect the May 2007 version of this clause.

B. Attachment J-1, Performance Work Statement, is revised to reflect updated IT security requirements resulting from the action delineated in "A" above and to reflect Revision A to NPR 2810, Security of Information Technology. These changes delineate NPR 2810.1A for each reference.

C. Attachment J-2, Data Procurement Document, is revised to incorporate the following documents:

974SE-003, Contractor Information Technology Security Program Plan
974SE-004, Information Technology (IT) Security Requirements Compliance Report(s)

As a result of this action, the following DRD is hereby deleted:

974CD-001, Information Technology Security Plan

D. Attachment J-10, Applicable Regulations and Procedures, is revised in order to reflect the incorporation of additional documents or revisions to current documents referenced in the Data Requirements delineated in "C" above. The added documents are as follows:

FIPS 199	*Standards for Security Categorization of Federal Information and Information Systems*
FIPS 200	*Minimum Security Requirements for Federal Information and Information Systems*
NIST SP 800-18	*Guide for Developing Security Plans for Federal Information Systems*
NIST SP 800-26	*Security Self-Assessment Guide for Information Technology Systems*
NIST SP 800-30	*Risk Management Guide for Information Technology Systems*
NIST SP 800-34	*Contingency Planning Guide for Information Technology Systems*
NIST SP 800-37	*Guide for the Security Certification and Accreditation of Federal Information Systems*
NIST SP 800-53	*Recommended Security Controls for Federal Information Systems*
NIST SP 800-61	*Computer Security Incident Handling Guide*

The following document is revised to reflect the current version:

NPR 2810.1A *Security of Information Technology*

E. It is mutually agreed that the changes delineated above are accomplished within the existing contract value and will not require an adjustment to that amount.

F. The modification(s) made above are reflected in total on the change page(s) enclosed herewith. In order to reflect the change(s) made, the page(s) listed below are hereby deleted from, or added to, NNM04AA02C. Changes are indicated in either bolded text or by a vertical line in the right margin to indicate the specific area(s) of change.

Page(s) Deleted	Page(s) Added
I-4	I-4
J-1-12	J-1-12
J-1-22	J-1-22
J-1-23	J-1-23
J-1-32	J-1-32
J-1-33	J-1-33
J-1-39	J-1-39
J-1-56	J-1-56
J-1-58	J-1-58
J-1-62	J-1-62
J-1-75	J-1-75
J-2-3	J-2-3
J-2-9	J-2-9
J-2-10	J-2-10
N/A	J-2-51 – 54
J-10-2 and 3	J-10- 2 and 3
J-10-18	J-10-18

G. All other terms and conditions of NNM04AA02C remain unchanged.

Clause No.	Title
52.242-4	Certification of Final Indirect Cost (Jan 1997)
52.242-10	F.o.b Origin- Government Bills of Lading or Prepaid Postage (Apr 1984)
52.242-13	Bankruptcy (Jul 1995)
52.243-2	Changes -- Cost-Reimbursement (Aug 1987) -- Alternate II (Apr 1984)
52.244-2	Subcontracts (Aug 1998) -- Alternate I (Aug 1998)[Insert "See Clause H.8" in (e) and "N/A" in (k)]
52.244-5	Competition in Subcontracting (Dec 1996)
52.244-6	Subcontracts for Commercial Items (Feb 2006)
52.245-5	Government Property (Cost-Reimbursement, Time-and-Materials, or Labor-Hour Contracts) (Jun 2003) DEVIATION (Jul 1995)
52.246-25	Limitation of Liability - Services (Feb 1997)
52.247-1	Commercial Bill of Lading Notations (Apr 1984)
52.247-67	Submission of Commercial Transportation Bills to the General Services Administration for Audit (Jun 1997)
52.249-6	Termination (Cost-Reimbursement) (Sep 1996)
52.249-14	Excusable Delays (Apr 1984)
52.251-1	Government Supply Sources (Apr 1984)
52.251-2	Interagency Fleet Management System Vehicles and Related Services (Jan 1991)
52.252-6	Authorized Deviations in Clauses (Apr 1984)
52.253-1	Computer Generated Forms (Jan 1991)

B. NASA/FAR SUPPLEMENT (48 CFR CHAPTER 18) CLAUSES

Clause No.	Title
1852.204-75	Security Classification Requirements (Sep 1989)[Insert "Top Secret" and "J-11"]
1852.204-76	Security Requirements for Unclassified Information Technology Resources **(May 2007)**
1852.215-84	Ombudsman (Oct 2003)[Insert "Robin N. Henderson, DE01, George C. Marshall Space Flight Center, MSFC, AL 35812, telephone (256) 544-1919, fax (256) 544-7920, email Robin.N.Henderson@nasa.gov"]
1852.216-89	Assignment and Release Forms (Jul 1997)
1852.219-74	Use of Rural Area Small Businesses (Sep 1990)
1852.219-75	Small Business Subcontracting Reporting (May 1999)
1852.219-76	NASA 8 Percent Goal (Jul 1997)
1852.219-77	NASA Mentor-Protégé' Program (May 1999)
1852.219-79	Mentor Requirements and Evaluation (Mar 1999)
1852.223-70	Safety and Health (Apr 2002)

a. Maintain and administer a NASA COMSEC account through the TOP SECRET/Sensitive Compartmented Information LEVEL, and provide encryption key management services, and classified documentation storage.
b. Provide encryption key management services, and store sensitive documentation for teleconferencing and data circuits.
c. Operate and maintain secure communications equipment to include voice, data, and video equipment.
d. Provide support for NASA National Security Systems.

2.7.2 IT Security Program

The contractor shall prepare ***a Contractor Information Technology Security Program Plan in accordance with DRD 974SE-003*** that documents ***the contractor's approach for implementing an information technology security program and which addresses the management, operational, and technical aspects of protecting the confidentiality, integrity and availability of information and information technology systems.*** The contractor shall ***assist with system security life-cycle development planning, support security certification and accreditation, and implement management, operational, and technical security controls for each general support computer system and major software application managed by contractor and subcontractor personnel in the performance of the contract in accordance with*** NPR 2810.1A, ***and shall comply with reporting requirements of DRD 974SE-004.***

2.7.3 Continuity of Services and Operations

The contractor shall develop, maintain, and test service continuity, contingency, and disaster recovery plans for all systems for which they are responsible. In support of disaster preparedness and recovery, the contractor shall:

a. Develop and maintain a Disaster Recovery Plan (DRD 974MA-007) to ensure the orderly recovery from a disaster that may render all or part of information facilities, systems, and equipment inoperable. This plan shall be in accordance with applicable NASA policy (NPR 1040.1).
b. Coordinate with information systems and disaster recovery experts across MSFC and NASA to verify integration of procedures and planning techniques.
c. Execute effective measures to protect all systems equipment and data from potential environmental threats.
d. After the occurrence of a disaster, ensure that systems are operational and restore any lost capabilities and data.
e. Develop and maintain a Continuity of Operations Plan in accordance with DRD 974MA-007.

3.2 DIGITAL TELEVISION (DTV)

The contractor shall support the NASA DTV Project. Support to the project shall include project management, design and engineering, operations, intercenter and intracenter coordination, implementation, and sustaining engineering directly related to the DTV Project. In providing this service, the contractor shall:

a. Provide customer support, such as collecting television requirements and preparing data in appropriate formats (DRD 974MA-007).
b. Develop transition and implementation plans (DRD 974MA-007).
c. Develop a laboratory to test equipment, interfaces, and processes.
d. Provide a technical interface with vendors, broadcast, and commercial television communities.
e. Provide engineering and operation expertise for consulting on distribution of audio and video between NASA Centers, within the centers, and to the media.
f. Coordinate Agency DTV implementation.
g. Coordinate, organize, and participate in technical working groups.
h. Support DTV flight projects.

3.3 IT SECURITY

The contractor shall provide IT Security services to the Agency customers. These services include maintenance of existing capabilities, development or acquisition, and implementation of enhancements. In providing these services, the contractor shall:

a. Utilize NASA's IT and wide area network capabilities to perform the support functions at all field centers and Headquarters.
b. Ensure that all IT resources and components are secured to minimum requirements in accordance with NPR 2810.1A and shall react to deal with any vulnerabilities or security incidents that might occur. This includes threat notification responses, risk management, network monitoring, centralized database collections, security response tracking and analysis, and forensics of IT Security activities. The contractor shall work closely with the NASA Center IT Security Managers or their representatives at all Centers.
c. Establish and maintain contact with internal and external technical working groups to include IT and IT security professional associations, NASA field centers, vendors, other government agencies, and national/international industry organizations.
d. Evaluate, develop, and test prototypes of IT security tools, techniques, and training.
e. Recommend, assist as needed in design, implement and maintain a firewall architecture/design that meets the NASA IT Security standards for perimeter architecture and Agencywide projects and networks.
f. Ensure that all personnel requiring access to DoD Classified information or networks have a minimum of a final Secret Security clearance or higher.

g. Establish and maintain an Agency IT Security Program and Response Center.
h. Conduct yearly IT Security risk assessments of Agency systems and services, in accordance with NPR 2810.1A.
i. Develop, implement and maintain a database to collect information on hostile probes throughout the Agency. Provide reports for trending analysis (DRD 974MA-006).

3.3.1 Intrusion Detection/Incident Response

The contractor shall provide early warning and detection of intrusions into the NASA wide area network through analysis of network traffic from IP Networks, including the Internet and key signatures associated with known vulnerabilities and cyber attacks. The contractor shall provide the response mechanism to contain, analyze and report on the number, source and nature of hostile probes coming from the networks, which includes the Internet. The contractor shall analyze and be able to project evolving situations based on data collected from contractor-managed networked and monitoring devices, as well as NASA-managed networked and monitoring devices. The contractor shall support NASA incident investigations. The contractor shall provide monthly reports on the nature of the NASA traffic passing through the NASA connections to any connections between NASA and its partners even if they are utilizing NASA address space, including Internet connections (DRD 974MA-006). The contractor shall support the deployment of network monitoring devices which would include the installation of network taps as required by NASA and the deployment of monitoring devices and data gathering systems to be housed in the contractor network and communications space as provide under or acquired through this contract.

3.3.2 NASA National Security Systems

The contractor shall provide support for secure intra- and inter-Agency communications within the Government that are necessary to improve distribution of threat information and coordination of disaster response. This shall include the provisioning, maintenance, and utilization of the NASA Secure Network and other National Security Systems.

The contractor shall install, maintain, and prepare designs for and operate the systems associated with the National Security systems. However, due to the nature of the classification and accreditation of these U.S. Government systems, any activity in this regard will require the Agency's approval before proceeding.

3.3.3 NASA Secure Sensitive but Unclassified Networks

The contractor shall support the deployment and operation of network encryption services such as VPN or point-to-point solutions. The contractor shall provide recommendations on how to support out of band management of IT security monitoring, data analysis engines firewall and VPN services and the operations and maintenance for such devices.

The contractor shall provide operations, sustaining engineering and maintenance of the mission video distribution system. In providing mission video, the contractor shall:

a. Operate and maintain the Goddard TV Central Facility, 8:00 am to 5:00 pm, Eastern Time, Monday through Friday, at the NASA Information Category Level of "Mission (MSN)," as defined in NPR 2810.1A. During Shuttle mission support, the facility is operated 24 hours per day, 7 days per week.
b. Record, edit, duplicate, and playback video for Agency programmatic activities.
c. Provide switching and distribution of video feeds and transponder switching of NASA Select TV service.
d. Provide on-site coverage during mission critical periods.
e. Document all operations, engineering, maintenance and repair activities, including a daily log, in accordance with DRD 974MA-006.
f. Coordinate and interface with government and contractor personnel regarding mission video activities.

3.6.4 Voice Services

The contractor shall provide voice teleconferencing and dedicated voice services.

3.6.4.1 Voice Teleconferencing Services (VoTS)

The contractor shall provide voice teleconferencing services to all COTR-designated locations. The contractor shall provide multiple levels of VoTS, such as:

- Dial-out service, where an operator calls all VoTS participants at a pre-arranged time.
- Dial-in service, where participants dial into a bridge and enter a passcode.
- On-demand conferencing, where a user is either assigned a unique account and passcode that can be distributed to participants or the user may contact an operator who will dial the participants.

The contractor shall provide:

a. Operator-based and web-based reservation and scheduling function so users may reserve the resources and specify details about their conferences (DRD 974MA-006).
b. Capability for operators to monitor in-progress calls and technical support and/or monitor conference quality.
c. Capability to record and transcribe conferences if requested by the call leader.
d. Monthly VoTS usage and cost summaries by NASA center (DRD 974MA-006).

e. Secure voice teleconferencing capability to COTR-designated locations.

3.6.4.2 VoTS Facilities

The contractor shall design, install, and maintain voice teleconferencing facilities at COTR-designated locations. The facility provision shall include:

a. Associated hardware and software systems.
b. Room layout, including coordination of facility changes (DRD 974MA-007).
c. Audio equipment.
d. Room operations panel.

3.6.4.3 Dedicated (Mission) Voice Service

The contractor shall provide transmission, bridging, and switching to support a system of dedicated, mission voice circuits working in conjunction with Center switching/conferencing systems to create inter-connected voice communications loops. The voice loops interconnect the different Center voice distribution systems that support diverse missions within the Agency. The contractor shall provide operations, sustaining engineering, and maintenance of the Voice Switching System (VSS). In providing this service, the contractor shall:

a. Operate and maintain the VSS 24 hours per day, 7 days per week, at the NASA Information Category Level of "Mission (MSN)," in accordance with NPR 2810.1**A.**
b. Operate the VSS and associated equipment in accordance with all applicable NISN Security Guidelines and Operating Procedures.
c. Provide fault isolation, restoration, testing, and monitoring, including detection of circuit degradation, of all the voice circuits terminated in the VSS.
d. Establish, maintain, and monitor voice conferences to NASA network and mission control centers and various other NASA, federal government and international partner facilities.
e. Provide on-site coverage during mission critical periods.
f. Coordinate and interface with government and contractor personnel regarding mission voice requirements-.

3.6.5 Data Services

The contractor shall provide routed data, dedicated data, and high rate data/video services.

3.6.5.1 Routed Data Services

The contractor shall provide the hardware, software, routing, management, and operations necessary to support NASA's routed data requirements. The contractor

a. Staff and maintain the control capability that is operational 24 hours per day 7 days per week at the NASA Information Category Level of "Mission (MSN)," as defined in NPR 2810.1A.
b. Provide configuration of high speed, wideband and video transport systems to meet specific mission requirements.
c. Coordinate with the government and interface with other contractors in accordance with government guidance.

3.7.3.4 Domain Name Service (DNS)

The contractor shall provide systems engineering and sustaining engineering support functions for NASA's DNS systems, at the domain level of nasa.gov. In performance of this function, the contractor shall:

a. Provide name registration for systems at the nasa.gov domain.
b. Provide sub-delegation to networks required to join NASA's network domain; e.g., msfc.nasa.gov.
c. Provide updated security patches and updates to nasa.gov DNS servers.

3.7.4 Problem Management

The contractor shall maintain systems and processes to respond to service problems detected by the contractor or their vendors or to problems reported by users. The contractor shall provide:

a. A capability to automatically route calls to appropriate control center operators. This capability shall include dedicated voice communications lines (e.g., orderwires) between control centers.
b. User-initiated and supplier-initiated problem reporting and resolution processes (DRD 974MA-006).
c. Escalation procedures and contacts for the contractor and the suppliers (DRD 974MA-007).
d. Automatic tracking and logging of customer trouble calls (DRD 974MA-006).
e. Processes, criteria, and point of contact (including other services providers and suppliers) necessary for effecting problem resolution (DRD 974MA-007).
f. A knowledge management capability to assist in resolution of troubles on the first call and to identify trends.
g. Call status metrics such as caller queue times and abandoned calls (DRD 974MA-006).
h. Real-time fault isolation and restoration of failed services, including coordination with carriers.
i. Maintain a daily log of installation trouble shooting and restoration activities (DRD 974MA-006).

4.1.3 Technical Architecture

The contractor shall define, implement, and maintain the IEMP technical architecture and coordinate with the Agency CIO to insure that the IEMP architecture is compliant with the overall Agency IT architecture (DRD 974MA-007). The contractor shall annually assess future directions and developments in information technology to insure that the IEMP architecture evolves to take advantage of new product releases by software and hardware vendors.

4.1.3.1 Integration Architecture

The contractor shall maintain and enhance the IEM integration architecture, which is based on EAI technology. The contractor shall provide and utilize a methodology that takes advantage of the EAI technology to shorten interface development timelines and reduce long-term maintenance costs. The contractor shall ensure that the integration architecture and associated product set supports evolving standards and technologies and is positioned to support NASA's ability to conduct electronic commerce with its customers and trading partners.

4.1.3.2 Information Delivery Architecture

The contractor shall maintain the IEMP reporting and information delivery architecture to be utilized for each module. As additional applications are implemented, the contractor shall evolve the architecture to incorporate SAP and non-SAP data into the data warehouse. The contractor shall establish a metadata management process for the information stored in the Business Information Warehouse (BW).

4.1.3.3 Security Architecture

The contractor shall support security certification and accreditation and implement required management, operational, and technical security controls for the underlying infrastructure components in accordance with NPR 2810.1A. The contractor shall also interact with NASA and contractor IT Security personnel in the review and audit of these documents and associated security activities such as risk assessments and intrusion detection exercises.

4.1.3.4 Systems Architecture

The contractor shall develop and maintain the technical infrastructure that is common across all module projects. Examples of infrastructure elements include: backup/recovery systems, storage systems, EAI components, data center networks/firewalls, and systems management/monitoring tools. The contractor shall design the infrastructure in a manner that maximizes systems management efficiencies and cost savings thereby reducing the operational costs while increasing customer satisfaction.

974MA-007). *The contractor shall assist with security life-cycle development planning, support security certification and accreditation, and implement management, operational, and technical security controls in accordance with NPR 2810.1A.*

4.2.1.3 Business and Application Architectures

Working with each module's process team, the contractor shall update and maintain the IEMP Business and Application architectures as described in sections 4.1.1 and 4.1.2 to reflect the Agency Design as approved by the module project steering committee (DRD 974MA-007).

4.2.1.4 Agency Interfaces

During the Agency Design phase, Agency Interfaces are identified and developed. Agency interfaces are interfaces between the IEM module and other Agency systems. The contractor shall define and follow a development methodology for interface development. The contractor shall lead the identification of Agency interface requirements, coordinate the functional design and requirements analysis process, develop the necessary technical designs, and develop all software components that must be built in the new IEM module or in the EAI tool. The contractor shall coordinate with the implementation contractor to insure that this development method integrates with the module project's implementation methodology and schedule. The contractor shall conduct unit testing and end-to-end testing of all interfaces before migrating the interfaces to system integration testing.

4.2.1.5 Extensions and Bolt-Ons

During Agency Design, the module project process team and implementation contractor may identify certain gaps that exist between the selected COTS product's base functionality and NASA's requirements. Options for addressing a gap include implementing a 3rd party COTS bolt-on that must be interfaced with the module or developing an extension in the COTS development environment. The contractor shall be responsible for developing any interfaces required between the module and selected bolt-ons. The contractor shall also be responsible for designing and developing any required extensions based on the functional designs delivered by the module project. The contractor shall conduct unit testing of any extensions and/or bolt-on interfaces before migrating these components to system integration testing.

4.2.1.6 Testing

The contractor shall support System Integration Testing for each individual module. Contractor representatives shall coordinate with each project during Agency Design to insure that the project's test plan includes the appropriate integration testing. The contractor shall support system integration testing by assisting testers with execution of Agency interfaces, bolt-on interfaces, extensions, and reports. The contractor shall also provide fixes for approved system discrepancies related to these components. The contractor shall provide the servers, databases and application instances to be utilized by the module projects in conducting unit, system, and integration testing. The contractor shall manage all security and system accounts required during the test phase (DRD

Center's readiness for implementation. After the contractor has completed testing of each application release, it shall stage all components (software, release notes, etc.) on the IEMP software distribution server and notify designated Center contacts of general availability.

4.3.3 Application Functional Support

The contractor shall perform application functional support for each module after completion of the implementation stabilization period. In providing this support, the contractor shall:

a. Possess detail application knowledge.
b. Perform software configuration tasks.
c. Generate queries and basic reports.
d. Develop and maintain security management processes ***in accordance with NPR 2810.1A.***
e. Provide Level II help desk support for the application.
f. Maintain end-user training plans and materials (DRD 974MA-007). The contractor shall maintain training materials and job aids that are used Agencywide. The Centers will be responsible for maintaining any Center-specific training materials.
g. Maintain the configuration tables that are defined as Agency configuration items.
h. Maintain all master data that is defined as centrally maintained.
i. Assess the impact of proposed changes to the baselined system.

4.3.4 Application Development Support

The contractor shall perform application development support for each module after completion of the implementation stabilization period. To accomplish this tasking, the contractor shall:

a. Use vendor-provided or other third-party tools to enhance the application.
b. Build extensions to the core software or augment with third party products.
c. Integrate the ERP solution with other applications or legacy systems.
d. Develop enhanced information delivery and reporting capabilities.
e. Assist in solving problems that relate to the technical characteristics of the ERP package.
f. Provide break/fix support for custom developed extensions, reports, and interfaces.

As a function of this support, the contractor shall define and implement a software release management strategy that incorporates enterprise requirements for change request, change control, and configuration management.

k. Schedule and operate the Contracting Officer's Technical Representative (COTR) designated video teleconferencing rooms.
l. Schedule the conference facilities located in Morris Auditorium, Conference Rooms P106, P110, and 815 in building 4200, and operate the facilities, including the audio/visual equipment.

5.5 INFORMATION TECHNOLOGY (IT) SECURITY SERVICES

The contractor shall provide IT Security services to the MSFC customers, including the NSSTC (an offsite facility in Huntsville). These services include maintenance of existing capabilities, development or acquisition, and implementation of enhancements. In providing these services, the contractor shall:

a. Ensure that all IT resources and components administered by the contractor are secured to minimum requirements in accordance with NPR 2810.1*A*.
b. Provide early warning, detection and resolution of vulnerabilities or security incidents. This includes threat notification responses, risk management, network monitoring, centralized database collections, security response tracking and analysis, and forensics of IT Security incidents.
c. Develop and test prototypes of IT security tools, techniques, and training.
d. Install and maintain firewalls for the MSFC and NSSTC private and public networks.
e. In concert with Agency requirements, manage and maintain secure authentication services for MSFC customers, including token-based and smart card services (see section 3.3.5).
f. Develop, evaluate, and test prototypes of IT security tools, techniques, and training specific to the MSFC and NSSTC environment.
g. ***Assist with system security life-cycle development planning, support security certification and accreditation, and other procedural/technical protective controls for MSFC and NSSTC IT resources.***
h. Assist with the implementation and administration of specific IT management disciplines, standards, and conventions as promulgated in Federal and Agency statutes, regulations, policies, procedures, administrative instructions, information bulletins, and directives.
i. Provide support for disaster recovery planning, contingency planning, vulnerability analysis, risk and exposure management, corrective action planning, sensitive disciplines, training, and reporting.
j. Provide rehabilitation support for IT resources impacted by hostile code or malicious software, including:
    1) Detection, validation and eradication services for MSFC and NSSTC information systems;
    2) Restoration of the system to its pre-infected configuration;
    3) Reallocation of resources to ensure the efficient and timely eradication of widespread infections.

National Aeronautics and Space Administration

PAGE REVISION LOG

DATA PROCUREMENT DOC.
NO. 974 ISSUE Basic

NOTE: The current revision is denoted by a vertical line in the outer margin adjacent to the affected text.

AS OF: 01-01-04

SUPERSEDING:

PAGE:

INSERT LATEST REVISED PAGES. DISCARD SUPERSEDED PAGES.

ITEM	PAGE	STATUS	ITEM	PAGE	STATUS
Mod 3	J-2-1				
Mod. 3	J-2-3				
Mod. 3	J-2-19				
Mod. 3	J-2-28				
Mod. 3	J-2-35				
Mod. 3	J-2-38				
Mod. 5	J-2-22				
Mod. 10	J-2-9				
Mod. 10	J-2-25				
Mod. 10	J-2-36				
Mod. 10	J-2-37-A				
Mod. 22	J-2-12				
Mod. 24	J-2-37-A				
Mod. 30	ALL				
Mod. 38	J-2-30				
Mod. 40	J-2-31				
Mod. 54	J-2-30				
Mod. 61	J-2-28				
Mod. 61	J-2-30				
Mod. 61	J-2-33				
Mod. 69	J-2-9				
Mod. 69	J-2-25 – J-2-28				
Mod. 69	J-2-38 – J-2-48				
Mod. 77	J-2-25				
Mod. 77	J-2-31				
Mod. 80	J-2-25				
Mod. 91	J-2-9				
Mod. 91	J-2-11				
Mod. 91	J-2-12 – 14				
Mod. 91	J-2-30				
Mod. 91	J-2-31				
Mod. 91	J-2-49 - 50				
Mod. 94	J-2-30				
Mod. 116	J-2-9 and 10				
Mod. 116	J-2-51 to 54				

MSFC - Form 3461-2 (Rev August 1970)

UNIFIED NASA INFORMATION TECHNOLOGY SERVICES (UNITeS)
Data Requirements List

DRD	DATA TYPE	TITLE	OPR
CD – Contractual Data			
974CD-001	2	Information Technology Security Plan **(DELETED)**	IS05
974CD-002	3	Badged Employee and Remote IT User Listing	AS50
974CD-003	3	Technology Reports (NFS 1852.227-70)	ED03
CM - Configuration Management			
974CM-001	2	Configuration Management Plan	ED43
LS – Logistics Support			
974LS-001	2	Government Property Management Plan	IS03
MA – Management			
974MA-001	1	Management Plan	IS01
974MA-002	2	Risk Management Plan, Analysis, and Tracking Reports	QD10
974MA-003	2	Major Information Systems Portfolio	IS01
974MA-004	2	Work Breakdown Structure (WBS) and WBS Dictionary	RS40
974MA-005	3	Financial Management Report (533M)	RS40
974MA-006	See DRD	Reports	IS01
974MA-007	See DRD	Documentation	IS01
974MA-008	3	Cost Reports	IS01
974MA-009	2/3	Export Control Plan and Reports	IS01
974MA-010	3	Contractor Self-Assessment Report	IS01
974MA-011	2	Certification of NISN Systems Readiness	IS01
974MA-012	3	Contractor UNITeS Status Review Report	IS01
974MA-013	3	Source/Destination Code Handbook	IS01
974MA-014	3	Mission Network Operations Logs (IPNOC and Conversion Devices)	IS01
974MA-015	3	Event Analysis and System Problem Resolution Report	IS01
RM – Reliability and Maintainability			
974RM-001	1	Operability/Maintainability Plan	IS01
SA – Safety			
974SA-001	2	On-site Safety and Health Plan	QD50
974SA-002	3	Mishap and Safety Statistics Reports	QD50
SE- Security			
974SE-001	3	Contractor Employee Clearance Document	AS50
974SE-002	3	Position Risk Designation for Non-NASA Employee Form	AS50
974SE-003	**2**	**Contractor Information Technology Security Program Plan**	**IS10**
974SE-004	**2**	**Information Technology (IT) Security Requirements Compliance Report(s)**	**IS10**

DATA REQUIREMENTS DESCRIPTION (DRD)

1. DPD NO.: 974 ISSUE: Basic
2. DRD NO.: **974CD-001**
3. DATA TYPE: 2
4. DATE REVISED: 8/15/07
5. PAGE: 1/1
6. TITLE: Information Technology Security Plan **(DELETED)**

7. **DESCRIPTION/USE:** To document information technology security risk management and safeguards for protection of unclassified NASA electronic information and data processed by Federal general support computer systems and major software applications.

8. **OPR:** IS05 9. **DM:** IS01

10. **DISTRIBUTION:** Per Contracting Officer's letter

11. **INITIAL SUBMISSION:** Draft with proposal

12. **SUBMISSION FREQUENCY:** Final 45 days after effective date of the contract

13. **REMARKS:** The information technology security plan(s) must be consistent with and further detail the approach contained in the offeror's proposal or sealed bid that resulted in the award of this contract and in compliance with the requirements stated in NFS 1852.204-76.
14. **INTERRELATIONSHIP:** PWS paragraphs 2.7.2, 4.1.3.3, 4.2.1.2, 4.3.3.d, 5.5.g

15. **DATA PREPARATION INFORMATION:**

15.1 SCOPE: Information Technology Security Plan(s) shall document the safeguards necessary to ensure sufficient availability, integrity, and confidentiality of that information accessed or managed within the systems and/or applications, based on the contractor's assessment of risks.

15.2 APPLICABLE DOCUMENTS:

NPG 2810.1	*Security of Information Technology*
NFS 1804.470-3	*Security Plan for unclassified Federal Information Technology systems*
NFS 1852.204-76	*Security Requirements for Unclassified Information Technology Resources*

15.3 CONTENTS: The Information Technology Security Plan shall meet the requirements of the applicable documents in 15.2 and document how the contractor and subcontractor personnel will utilize, in a secure manner commensurate with the sensitivity of the information involved, those Federal computer systems and software applications managed by others. The plan shall describe the contractor's processes for implementing information security including personnel background screening, personnel awareness and training, information protection, and security incident response.

Additionally, a separate system-level Information Technology System Security Plan shall be prepared for each Federal general support computer system or major software application managed by the contractor and/or subcontractor personnel in the performance of this contract. The Information Technology System Security Plan(s) shall meet the requirements of the applicable documents in 15.2. NPG 2810.1 defines "general support computer systems" and "major applications" and provides plan requirements for both.

15.4 FORMAT: Contractor format is acceptable.

15.5 MAINTENANCE: Changes shall be incorporated by change page or complete reissue.

DATA REQUIREMENTS DESCRIPTION (DRD)

1. DPD NO.: 974 ISSUE: Basic 2. DRD NO.: 974SE-003
3. DATA TYPE: 2 4. DATE REVISED:
5. PAGE: 1/2

6. TITLE: Contractor Information Technology Security Program Plan

7. DESCRIPTION/USE: To ensure that the contractor fully understands their responsibility for information and information technology (IT) security as required in NFS 1852.204-76. This plan shall describe the contractor's comprehensive information technology security program that addresses the management, operational, and technical aspects of protecting the confidentiality, integrity and availability of information and information technology systems.

8. OPR: IS10 9. DM: IS01

10. DISTRIBUTION: One copy each CO and COTR, on-line EDMS

11. INITIAL SUBMISSION: Final 30 days after contract award.

12. SUBMISSION FREQUENCY: Revise after any significant changes. Review and update every three years.

13. REMARKS: The Federal Information Processing Standards (FIPS) Publication Series of the National Institute of Standards and Technology (NIST) is the official series of publications relating to standards and guidelines adopted and promulgated under the provisions of the Federal Information Security Management Act (FISMA) of 2002. FIPS Pub 200, Minimum Security Requirements for Federal Information and Information Systems, which specifies minimum security requirements for information and information systems supporting the executive agencies of the federal government and a risk-based process for selecting the security controls necessary to satisfy the minimum security requirements.

The seventeen security-related areas to be addressed in the content of the Contractor IT Security Program Plan represent a broad-based, balanced information technology security program that addresses the management, operational, and technical aspects of protecting information and information technology systems. Additional information for these security-related areas can be found in FIPS Pub 200.

14. INTERRELATIONSHIP: PWS 2.7.2

15. DATA PREPARATION INFORMATION:

15.1 SCOPE: The extent of the Contractor IT Security Program Plan can vary and shall be appropriate to comply with the breadth of sensitivity level security requirements for protecting information and information technology (IT) when the Contractor or its subcontractors must obtain physical or electronic access to NASA's computer systems, networks, or IT infrastructure, or where information is stored, generated, processed or exchanged by/with NASA or on behalf of NASA by a contractor or subcontractor, regardless of whether the information resides on a NASA or a contractor/ subcontractor's information system.

DRD Continuation Sheet

TITLE: Contractor Information Technology (IT) Security Program Plan — DRD NO.: 974SE-003

DATA TYPE: 2 — PAGE: 2/2

15.2 APPLICABLE DOCUMENTS:

NFS 1852.204-76	*Security Requirements for Unclassified Information Technology Resources (May 2007)*
FIPS 200	*Minimum Security Requirements for Federal Information and Information Systems*

15. DATA PREPARATION INFORMATION:

15.3 CONTENTS: The Contractor IT Security Program Plan shall describe the contractor's comprehensive information technology security program that provides an approach to address each of the security-related areas (see Remarks) for protecting MSFC and Agency information and supported information technology systems.

1. Management.
   (a) Certification, Accreditation, and Security Assessments.
   (b) Planning.
   (c) Risk Assessment.
   (d) Systems and Services Acquisition.
2. Operational.
   (a) Awareness and Training.
   (b) Configuration Management.
   (c) Contingency Planning.
   (d) Incident Response.
   (e) Maintenance.
   (f) Media Protection.
   (g) Physical and Environmental Protection.
   (h) Personnel Security.
   (i) System and Information Integrity.
3. Technical.
   (a) Access Control.
   (b) Audit and Accountability.
   (c) Identification and Authentication.
   (d) System and Communications Protection.

NOTE: Any security-related area not currently implemented in the Contractor's IT security program shall be identified and the contractor's plan of action for implementation shall be explained.

15.4 FORMAT: Contractor format is acceptable and shall be consistent with contents of paragraph 15.3 of this DRD.

15.5 MAINTENANCE: Changes shall be incorporated by change page or complete reissue.

DATA REQUIREMENTS DESCRIPTION (DRD)

1. DPD NO.: 974 ISSUE: Basic 2. DRD NO.: **974SE-004**
3. DATA TYPE: 2 4. DATE REVISED:
5. PAGE: 1/2

6. **TITLE**: Information Technology (IT) Security Requirements Compliance Report(s)

7. **DESCRIPTION/USE**: To provide an overview of the Contractor's compliance with the IT security requirements in NFS 1852-204-76 and any additions/augmentations described in NPR 2810.1A. The contractor shall specify when IT systems or applications managed by the contractor are required to follow NASA Certification and Accreditation (C&A) processes as described in NPR 2810.1A, requiring the utilization of the MSFC system security documentation repository for the development and management of required documents. This report will be used in conjunction with all System security documentation as described in NPR 2810.1A to verify the contractor's compliance and shall be approved by their Organization Senior Management responsible for IT.

8. **OPR**: IS10 9. **DM**: IS01

10. **DISTRIBUTION**: One copy each CO and COTR, on-line EDMS

11. **INITIAL SUBMISSION**: 30 days after contract award.

12. **SUBMISSION FREQUENCY**: The report shall be reviewed and updated on a yearly basis.

13. **REMARKS**: The NFS 1852.204-76 identifies security requirements for IT Security and Physical and Logical Access for unclassified information technology resources. It specifically identifies IT security requirements that include the preparation of certain IT security documents that are included in the Security Accreditation package required for a National Institute of Standards and Technology (NIST) Certification and Accreditation (C&A) process (reference NIST 800-37). However, NFS 1852.204-76 does not require the Contractor to follow a formal NIST C&A process unless there are any additions/augmentations described in the NASA C&A processes established in NPR 2810.1A.

    The NFS 1852.204-76 requires the Contractor to submit to the Contracting Officer an IT Security Plan, Risk Assessment and FIPS 199 Assessment that shall be incorporated into the contract as compliance documents. Due to the critical sensitivity of the content of these documents, this IT Security Requirements Compliance Report shall be submitted to the Contracting Officer as evidence that these requirements have been met. Once approved by the MSFC IT Security Office, it will be maintained with the contract as a compliance document. Due to the nature of this contract, the IT System Security Plan, Risk Assessment and all other required system security documents shall be prepared and maintained by the contractor as required by NASA C&A processes described in NPR 2810.1A and be submitted into the MSFC system security documentation repository. These system security documents shall not be submitted directly to the Contracting Officer.

14. **INTERRELATIONSHIP**: PWS 2.7.2

DRD Continuation Sheet

TITLE: Information Technology (IT) Security Requirements Compliance Report(s) DRD NO.: 974SE-004

DATA TYPE: 2 PAGE: 2/2

15. DATA PREPARATION INFORMATION:

15.1 SCOPE: The IT Security Requirements Compliance Report shall specify when IT systems or applications managed by the contractor are required to follow NASA C&A processes requiring the utilization of the MSFC system security documentation repository, provide reference to policies and procedures required for compliance to IT security requirements, and provide dates of compliance and a statement of compliance to be signed by Organization Senior Management responsible for IT.

15.2 APPLICABLE DOCUMENTS:

FIPS 199	*Standards for Security Categorization of Federal Information and Information Systems*
NFS 1852.204-76	*Security Requirements for Unclassified Information Technology Resources (May 2007)*
NPR 2810.1A	*Security of Information Technology*
NIST SP 800-61	*Computer Security Incident Handling Guide*
NIST 800-37	*Guide for the Security Certification and Accreditation of Federal Information Systems*

15.3 CONTENTS: In response to the requirements of NFS 1852.204-76, the IT Security Requirements Compliance Report shall specify when IT systems or applications managed by the contractor are required to follow NASA C&A processes as described in NPR 2810.1A. It shall identify policies and procedures for Incident Response and Annual IT security training. It shall include a statement of compliance for: ensuring that incidents are reported per NIST SP 800-61 and that any confirmed incident for a system containing NASA information or controlling NASA assets is reported as required; providing NASA access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases, and personnel used in performance of the contract; ensuring contractor system administrator(s) have demonstrated appropriate knowledge; ensuring that NASA's Sensitive But Unclassified (SBU) information is encrypted in storage and transmission; completing contractor personnel screening requirements; ensuring the return of all NASA information and IT resources at contract completion as required; certifying that all NASA information has been purged from contractor-owned systems used in the performance of the contract; and ensuring the inclusion of NFS 1852.204-76 in all subcontracts, as required. The statement of compliance shall be signed by Organization Senior Management responsible for ensuring that IT requirements have been met.

The contractor shall indicate in the compliance statement when the contractor is located at a NASA Center or installation or is using NASA IP address space and ensure: compliance with processes for submitting requests for non-NASA provided external Internet connections to the Contracting Officer for approval by the NSCCB; compliance with NASA CIO metrics; and utilization of the NASA Public Key Infrastructure.

15.4 FORMAT: A template shall be provided by the MSFC IT Security Office (IS10).

15.5 MAINTENANCE: Changes shall be incorporated by change page or complete reissue.

NPD 2190.1	NASA Export Control Program
NPD 2220.5	Management of NASA Scientific and Technical Information (STI)
NPD 2530.1	Monitoring or Recording of Telephone or Other Conversations
NPD 2540.1	Use of Government Telephones
NPD 2570.5	Radio Frequency Spectrum Management
NPD 2800.1	Managing Information Technolgoy
NPD 2810.1	Security of Information Technology
NPD 2820.1	NASA Software Policies
NPD 4200.1	Equipment Management
NPD 4300.1	NASA Personal Property Disposal Policy
NPD 8610.6	Graphic Markings on Space Transportation Vehicles, U.S. Components of the International Space Station Component Systems, and Payloads
NPD 9501.1	NASA Contractor Financial Management Reporting System

NASA PROCEDURAL REGULATIONS

NPR 1040.1	NASA Continuity of Operations (COOP) Planning Procedures and Guidelines
NPR 1441.1	NASA Records Retention Schedules
NPR 1490.5	NASA Procedural Guidance for Printing, Duplication, and Copying Management
NPR 1600.1	**NASA Security Program Procedural Requirements w/Change**
NPR 1620.1	Security Procedures and Guidelines
NPR 2190.1	NASA Export Control Program
NPR 2200.2	Guidelines for Documentation, Approval, and Dissemination of NASA Scientific and Technical Information (STI)
NPR 2800.1	Managing Information Technology **(Mod No. 116)**

AN ASTERISK (*) INDICATES DOCUMENTS ARE RESTRICTED; THEY MAY BE VIEWED ON SITE. NO COPIES WILL BE ALLOWED OFF SITE.

NPR 2810.1A	Security of Information Technology
NPR 4100.1	NASA Materials Inventory Management Manual
NPR 4200.1	NASA Equipment Management Manual
NPR 4200.2	Equipment Management Manual for Property Custodians
NPR 4300.1	NASA Personal Property Disposal Procedures and Guidelines
NPR 7120.5	Program and Project Management Processes and Requirements
NPR 8715.3	NASA Safety Manual
NPR 9501.2	NASA Contractor Financial Management Reporting

MARSHALL POLICY DIRECTIVES

MSFC Directories are available from the Directives Master List on the MSFC Integrated Document Library: http://inside.msfc.nasa.gov/MIDL/

MPD 1040.3	MSFC Emergency Program
MPD 1280.1	Marshall Management Manual
MPD 1380.1	Release of Information to News and Information Media
MPD 1394.1	Control of Audiovisual Products
MPD 1800.1	MSFC Smoking Policy
MPD 1840.1	MSFC Environmental Health Program
MPD 1840.2	MSFC Hearing Conservation Program
MPD 2190.1	MSFC Export Control Program
MPD 2210.1J	Documentation Input andOutput of the MSFC Documentation Repository
MPD 2800.1	Management of Information Technology Systems and Services at MSFC **(Mod. No. 116)**

AN ASTERISK (*) INDICATES DOCUMENTS ARE RESTRICTED; THEY MAY BE VIEWED ON SITE. NO COPIES WILL BE ALLOWED OFF SITE.

OTHER

General Records Schedules are available from the National Archives and Records Administration home page, "Records Management – Publications" at http://www.nara.gov/records/index/html

INFORMATION TECHNOLOGY SECURITY

FIPS 199	Standards for Security Categorization of Federal Information and Information Systems
FIPS 200	Minimum Security Requirements for Federal Information and Information Systems
NIST SP 800-18	Guide for Developing Security Plans for Federal Information Systems
NIST SP 800-26	Security Self-Assessment Guide for Information Technology Systems
NIST SP 800-30	Risk Management Guide for Information Technology Systems
NIST SP 800-34	Contingency Planning Guide for Information Technology Systems
NIST SP 800-37	Guide for the Security Certification and Accreditation of Federal Information Systems
NIST SP 800-53	Recommended Security Controls for Federal Information Systems
NIST SP 800-61	Computer Security Incident Handling Guide

AN ASTERISK (*) INDICATES DOCUMENTS ARE RESTRICTED; THEY MAY BE VIEWED ON SITE. NO COPIES WILL BE ALLOWED OFF SITE.